Mensagem de erro Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:" com perda de ping sobre solução de problemas de túnel IPsec

Contents

Introduction

Este documento descreve como resolver a perda de ping em um túnel IPsec combinado com mensagens "%CRYPTO-4-RECVD_PKT_MAC_ERR" no syslog, como mostrado na caixa:

```
May 23 11:41:38.139 GMT: %CRYPTO-4-RECVD_PKT_MAC_ERR:
decrypt: mac verify failed for connection
id=2989 local=172.16.200.18 remote=172.16.204.18 spi=999CD43B
seqno=00071328
```

Uma pequena porcentagem dessas gotas é considerada normal. No entanto, uma alta taxa de queda por causa desse problema pode afetar o serviço e pode exigir a atenção do operador da rede. Observe que essas mensagens relatadas nos syslogs têm taxa limitada em intervalos de 30 segundos, portanto, uma única mensagem de log nem sempre indica que apenas um único pacote foi descartado. Para obter uma contagem precisa dessas quedas, emita o comando **show crypto ipsec sa detail** e examine o SA ao lado da ID de conexão vista nos registros. Entre os contadores SA, os **pkts verify failed** error counters contabilizam o total de descarte de pacotes devido à falha de verificação do código de autenticação da mensagem (MAC).

```
interface: GigabitEthernet0/1
Crypto map tag: MPLSWanGREVPN, local addr 172.16.204.18

protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.204.18/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (172.16.205.18/255.255.255.255/47/0)
current_peer 172.16.205.18 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 51810, #pkts encrypt: 51810, #pkts digest: 51810
```

```
#pkts decaps: 44468, #pkts decrypt: 44468, #pkts verify: 44468
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#pkts no sa (send) 0, #pkts invalid sa (rcv) 0
#pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
#pkts invalid prot (recv) 0, #pkts verify failed: 8
#pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
#pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (recv) 0

local crypto endpt.: 172.16.204.18, remote crypto endpt.: 172.16.205.18
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/1
current outbound spi: 0xD660992C(3596654892)

inbound esp sas:
spi: 0x999CD43B(2577191995)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2989, flow_id: AIM-VPN/SSL-3:2989, sibling_flags 80000006,
crypto map: MPLSWanGREVPN
sa timing: remaining key lifetime (k/sec): (4257518/24564)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE

outbound esp sas:
spi: 0xD660992C(3596654892)
transform: esp-3des esp-sha-hmac ,
in use settings ={Transport, }
conn id: 2990, flow_id: AIM-VPN/SSL-3:2990, sibling_flags 80000006,
crypto map: MPLSWanGREVPN
sa timing: remaining key lifetime (k/sec): (4199729/24564)
IV size: 8 bytes
replay detection support: N
Status: ACTIVE
```

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas em testes feitos com o Cisco IOS® versão 15.1(4)M4. Embora ainda não testados, os scripts e a configuração devem funcionar com versões anteriores do software Cisco IOS, já que ambos os miniaplicativos usam a versão 3.0 do EEM (que é suportada na versão 12.4(22)T ou superior do IOS).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informações do recurso

O "%CRYPTO-4-RECVD_PKT_MAC_ERR: descriptografar:" implica que um pacote criptografado foi recebido com falha na verificação MAC. Esta verificação é um resultado do conjunto de transformação de autenticação configurado:

```
Router (config)# crypto ipsec transform transform-1 esp-aes 256 esp-md5-hmac
```

No exemplo acima, *"esp-aes 256"* define o algoritmo de criptografia como AES de 256 bits, e *"esp-md5"* define o MD5 (variante HMAC) como o algoritmo de hash usado para autenticação. Algoritmos de hash como MD5 são normalmente usados para fornecer uma impressão digital do conteúdo de um arquivo. A impressão digital digital é frequentemente usada para garantir que o arquivo não tenha sido alterado por um invasor ou vírus. Assim, a ocorrência desta mensagem de erro geralmente implica:

- A chave errada foi usada para criptografar ou descriptografar o pacote. Esse erro é muito raro e pode ser causado por um bug de software.

-OU-

- O pacote foi adulterado durante o trânsito. Esse erro pode ser devido a um circuito sujo ou a um evento hostil.

Metodologia de solução de problemas

Como essa mensagem de erro é normalmente causada por corrupção de pacote, a única maneira de fazer uma análise de causa básica é usar o EPC para obter capturas de pacote completas do lado da WAN em ambos os pontos finais do túnel e compará-las. Antes de obter as capturas, é melhor identificar que tipo de tráfego dispara esses logs. Em alguns casos, pode ser um tipo específico de tráfego; em outros casos, ele pode ser aleatório, mas facilmente reproduzido (como 5-7 descartes a cada 100 pings). Nessas situações, o problema fica um pouco mais fácil de ser identificado. A melhor maneira de identificar o gatilho é marcar o tráfego de teste com marcas DSCP e capturar os pacotes. O valor de DSCP é copiado para o cabeçalho ESP e pode ser filtrado com o Wireshark. Essa configuração, que pressupõe um teste com 100 pings, pode ser usada para marcar os pacotes ICMP:

```
ip access-list extended VPN_TRAFFIC
 permit icmp <source> <destination>
class-map match-all MARK
 match access-group name VPN_TRAFFIC
policy-map MARKING
 class MARK
   set dscp af21
```

Essa política agora deve ser aplicada à interface de ingresso onde o tráfego claro é recebido no roteador de criptografia:

```
interface GigabitEthernet0/0
service-policy MARKING in
```

Como alternativa, você pode executar esse teste com o tráfego gerado pelo roteador. Para isso, você não pode usar a Qualidade de Serviço (QoS) para marcar os pacotes, mas pode usar o Roteamento Baseado em Políticas (PBR - Policy-Based Routing).

Note: Para localizar marcas críticas (5) de DSCP, use o filtro do Wireshark **ip.dsfield.dscp == 0x28**.

```
ip access-list extended VPN_TRAFFIC
 permit icmp <source> <destination>
route-map markicmp permit 10
match ip address vpn
set ip precedence critical
ip local policy route-map markicmp
```

Depois que a marcação de QoS for configurada para o tráfego ICMP, você poderá configurar a captura de pacotes embutidos:

```
Router(config)# ip access-list ext vpn_capo
Router(config)# permit ip host
```

```
Router(config)# permit ip host
```

```
Router(config)#  exit //the capture is only configured in enable mode.
Router# monitor capture buffer vpncap size 256 max-size 100 circular
Router# monitor capture buffer vpncap filter access-list vpn_capo
Router# monitor capture point ip cef capo fastEthernet 0/1 both
Router# monitor capture point associate capo vpncap
Router# monitor capture point start capo //starts the capture.
To stop replace the "start" keyword with "stop"
```

Note: esse recurso foi apresentado no Cisco IOS versão 12.4(20)T. Consulte Captura de Pacotes Incorporados para obter mais informações sobre EPCs.

O uso de uma captura de pacote para solucionar esse tipo de problema exige que o pacote inteiro seja capturado, não apenas uma parte dele. O recurso EPC nas versões do Cisco IOS anteriores a 15.0(1)M tem um limite de buffer de 512K e um limite máximo de tamanho de pacote de 1024 bytes. Para evitar essa limitação, atualize para 15.0(1)M ou código mais recente, que agora suporta um tamanho de buffer de captura de 100M com um tamanho máximo de pacote de 9500 bytes.

Se o problema puder ser reproduzido com confiabilidade a cada ping de contagem de 100, o pior cenário é programar uma janela de manutenção para permitir apenas o tráfego de ping como um teste controlado e fazer as capturas. Esse processo deve levar apenas alguns minutos, mas interrompe o tráfego de produção por esse tempo. Se você usar a marcação de QoS, poderá eliminar a exigência de restringir pacotes somente a pings. Para capturar todos os pacotes de ping em um buffer, você deve garantir que o teste não seja realizado durante as horas de pico.

Se o problema não for facilmente reproduzido, você poderá usar um script EEM para automatizar a captura de pacotes. A teoria é que você começa as capturas de ambos os lados em um buffer circular e usa EEM para interromper a captura de um lado. Ao mesmo tempo, o EEM interrompe a captura, faça com que envie uma armadilha snmp para o peer, que interrompe sua captura. Esse

processo pode funcionar. Mas se a carga for pesada, o segundo roteador pode não reagir com a rapidez suficiente para interromper sua captura. É preferível um teste controlado. Aqui estão os scripts do EEM que implementarão o processo:

```
Receiver
========
event manager applet detect_bad_packet
event syslog pattern "RECVD_PKT_MAC_ERR"
action 1.0 cli command "enable"
action 2.0 cli command "monitor capture point stop test"
action 3.0 syslog msg "Packet corruption detected and capture stopped!"
action 4.0 snmp-trap intdata1 123456 strdata ""
```

```
Sender
======
event manager applet detect_bad_packet
event snmp-notification oid 1.3.6.1.4.1.9.10.91.1.2.3.1.9.
oid-val "123456" op eq src-ip-address 20.1.1.1
action 1.0 cli command "enable"
action 2.0 cli command "monitor capture point stop test"
action 3.0 syslog msg "Packet corruption detected and capture stopped!"
```

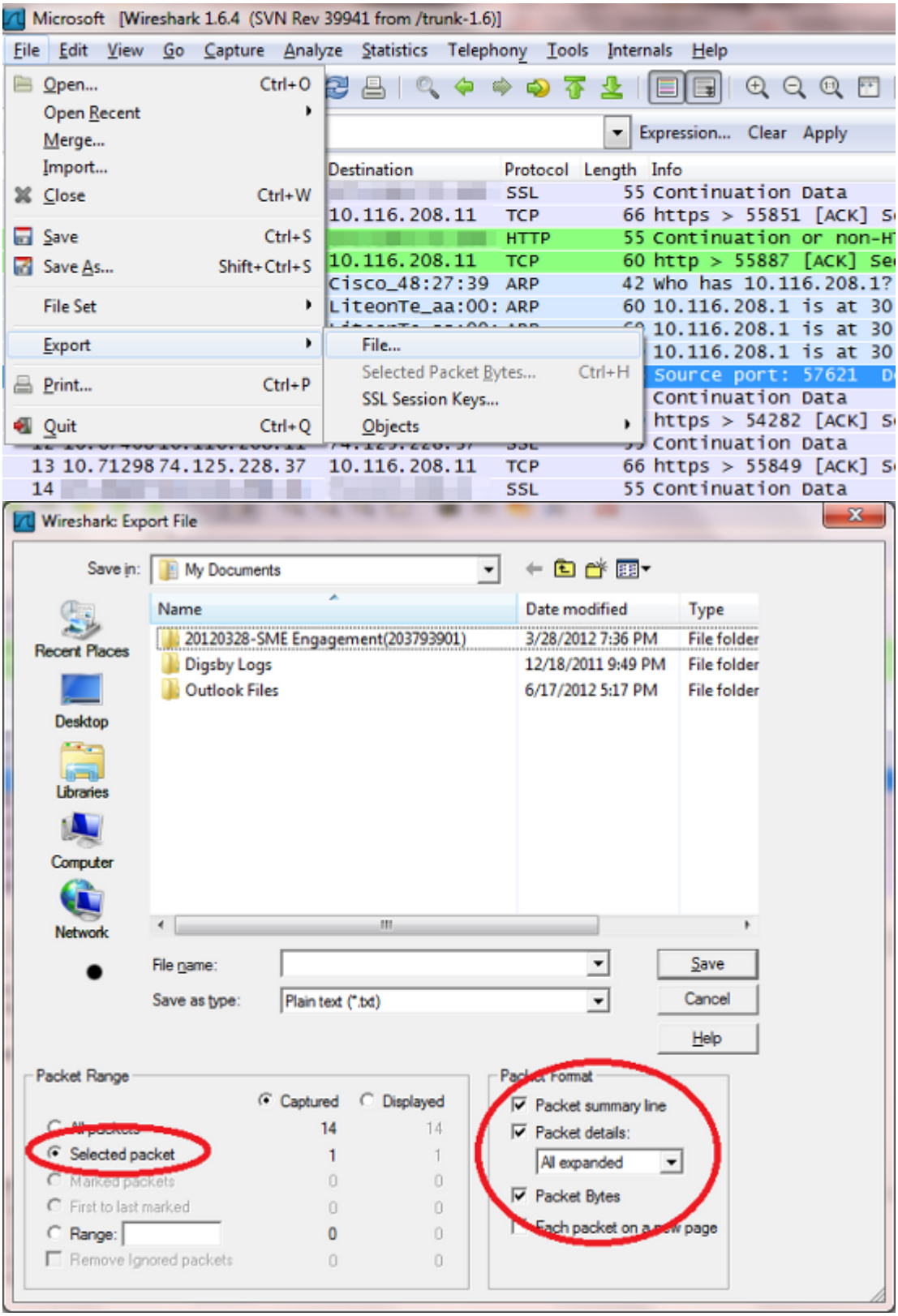
Observe que o código na caixa anterior é uma configuração testada com 15.0(1)M. Talvez você queira testá-la com a versão específica do Cisco IOS que seu cliente usa antes de implementá-la no ambiente do cliente.

Análise de dados

1. Quando as capturas tiverem sido concluídas, use o TFTP para exportá-las para um PC.
2. Abra as capturas com um analisador de protocolo de rede (como o Wireshark).
3. Se a marcação QoS tiver sido usada, filtre os respectivos pacotes.

   ```
   ip.dsfield.dscp==0x08
   ```

   "0x08" é específico para o valor de DSCP AF21. Se um valor de DSCP diferente for usado, o valor correto pode ser obtido da própria captura de pacote ou da lista de valores de DSCP do gráfico de conversão. Consulte DSCP e Valores de Precedência para obter mais informações.
4. Identifique o ping descartado nas capturas do remetente e localize esse pacote nas capturas no lado do receptor e do remetente.
5. Exporte esse pacote de ambas as capturas como mostrado nesta imagem:



6. Faça uma comparação binária dos dois. Se forem idênticos, não houve erros em trânsito e o Cisco IOS lançou um falso negativo na extremidade de recebimento ou usou a chave errada na extremidade do remetente. Em ambos os casos, o problema é um bug do Cisco IOS. Se os pacotes forem diferentes, os pacotes foram violados na transmissão.

   Aqui está o pacote que deixou o mecanismo de criptografia no FC:

```
*Mar  1 00:01:38.923: After encryption:
05F032D0: 45000088 00000000 E.......
05F032E0: FF3266F7 0A01201A 0A012031 7814619F .2fw.. ... 1x.a.
05F032F0: 00000001 DE9B4CEF ECD9178C 3E7A7F24 ....^.LolY..>z.$
```

```
05F03300: 83DCF16E 7FD64265 79F624FB 74D5AEF2 .\qn.VBeyv${tU.r
05F03310: 5EC0AC16 B1F9F3AB 89524205 A20C4E58 ^@,.1ys+.RB.".NX
05F03320: 09CE001B 70CC56AB 746D6A3A 63C2652B .N..pLV+tmj:cBe+
05F03330: 1992E8AF 2CE2A279 46367BDB 660854ED ..h/,b"yF6{[f.Tm
05F03340: 77B69453 83E47778 1470021F 09436285 w6.S.dwx.p...Cb.
05F03350: CB94AEF5 20A65B1F 480D86F6 125BA12E K..u &[.H..v.[!.
```

Aqui está o mesmo pacote que foi recebido no peer:

```
4F402C90:                   45000088 00000000          E.......
4F402CA0: FF3266F7 0A01201A 0A012031 7814619F .2fw.. ... 1x.a.
4F402CB0: 00000001 DE9B4CEF ECD9178C 3E7A7F24 ....^.LolY..>z.$
4F402CC0: 83DCF16E 7FD64265 79F624FB 74D5AEF2 .\qn.VBeyv${tU.r
4F402CD0: 5EC0AC16 B1F9F3AB 89524205 A20C4E58 ^@,.1ys+.RB.".NX
4F402CE0: 09CE001B 70CC56AB 00000000 00000000 .N..pLV+........
4F402CF0: 00000000 00000000 00000000 00000000 ................
4F402D00: 00000000 00000000 00000000 00000000 ................
4F402D10: 00000000 00000000 00000000 00000000 ................
```

Nesse ponto, é mais provável que seja um problema do ISP e esse grupo deve estar envolvido na solução de problemas.

Problemas comuns

- O bug da Cisco ID CSCed87408 descreve um problema de hardware com o mecanismo de criptografia nos 83xs, onde os pacotes de saída aleatórios são corrompidos durante a criptografia, o que leva a erros de autenticação (nos casos em que a autenticação é usada) e quedas de pacotes na extremidade de recebimento. É importante perceber que você não verá esses erros no próprio 83x, mas no dispositivo receptor.

- Às vezes, os roteadores que executam código antigo mostram esse erro. Você pode atualizar para as versões de código mais recentes, como 15.1(4) M4, para resolver o problema.

- Para verificar se o problema é de hardware ou software, desative a criptografia de hardware. Se as mensagens de log continuarem, será um problema de software. Caso contrário, uma RMA deve resolver o problema.
  Lembre-se de que se você desabilitar a criptografia de hardware, ela poderá causar grave degradação da rede para túneis VPN com carga elevada. Portanto, a Cisco recomenda que você tente os procedimentos descritos neste documento durante uma janela de manutenção.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems